UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/584,293	06/23/2006	Jari Arkko	3772-32	8960

23117 7590 04/25/2008
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
DOAN, PHUOC HUU	

ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
04/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/584,293	ARKKO ET AL.	
	Examiner	Art Unit	
	PHUOC H. DOAN	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *31-60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *31-52* is/are allowed.

6)☒ Claim(s) *53-60* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claims 53, and 55 are objected to because of the following informalities:

As to claim 53, the claim recited such as "authenticating the mobile node to the second access node **using the method of any one of the preceding claims**". The high light above is indicated improper of the independent claim, because the independent claim can not use "of any one of the preceding claims".

As to claim 55, claim 1 has been cancelled, therefore, it could not dependency on the cancelled claim.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 53-56 are rejected under 35 U.S.C. 102(e) as being anticipated by Sharma (US Pub No: 2003/0031151).

As to claim 53, Sharma discloses a method of authenticating a mobile node when roaming with a communication system (page 4, par. [0054-0055] "based on the authentication, the mobile device roaming from GPRS to WLAN"), the method comprising: following handover of the mobile node from a first access node of the communication system to a second access, authenticating the mobile node to the second access node (page 4, par. [0055], [0056] "the mobile device roaming or handover from GPRS first access node to WLAN second access node are required the authentication").

As to claim 54, Sharma further discloses wherein the mobile node has been previously authenticated to the said communication system by a home network of the mobile node (page 4, par. [0059]).

As to claim 55, Sharma further discloses the method comprising: providing a first authentication key K sub s0 for use by the mobile node and a first access node (page 4, par. [0055]); sending a hash of the first authentication key hash(K sub s0) to a second access node and the mobile node; and generating a new authentication key K sub s1 in accordance with the hash hash(K sub s0) (See page 5, par. [0075]).

As to claim 56, claim is rejected for the same reason as set forth in claim 55.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 57-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sharma in view of Chow (US Pub No: 2002/0002678).

As to claim 57, Sharma does not disclose further comprising the steps of: exchanging a first nonce N.sub.C1 provided by the mobile node and a second nonce N.sub.A1 provided by the second access node between the mobile node and the second access node; and wherein the new authentication key K.sub.S1 is generated in accordance with the hash of the first session key K.sub.S0 the first nonce N.sub.C1 and the second nonce N.sub.A1 in accordance with the function K.sub.S1=hash(hash(K.sub.S0), N.sub.C1, N.sub.A1).

In the same filed of endeavor, Chow discloses 57. A method according to claim 55, further comprising the steps of: exchanging a first nonce N.sub.C1 provided by the mobile node and a second nonce N.sub.A1 provided by the second access node between the mobile node and the second access node (page 2, par. [0025-0026]); and wherein the new authentication key K.sub.S1 is generated in accordance with the hash of the first session key K.sub.S0 the first nonce N.sub.C1 and the second nonce N.sub.A1 in accordance with the function K.sub.S1=hash(hash(K.sub.S0), N.sub.C1, N.sub.A1) (See page 2 through page 3, par. [0032-0038] "the authentication key based on the hash with the value to calculate and assigned between two access node which indicated the first computer program 10, and the second computer program 12").

As to claim 58, Sharma discloses a mobile wireless terminal, the terminal comprising means for generating and storing a first numerical chain comprising a series of n values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value (page 5 par. [0062-0063], [0075] "MD-5 hash transforms it into a unique 128 bit value"); and means for disclosing values from the numerical chain to

an access node in order to allow the access node to authenticate the mobile wireless terminal (page 5, par. [0072-0075]). However, Sharma does not disclose the subsequent value is not easily obtainable from that given value, a series of n values using a one-way coding function.

In the same field of invention, Chow discloses the subsequent value is not easily obtainable from that given value (page 9, par. [0149-0156], a series of n values using a one-way coding function (page 9, par. [0165-0166]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the subsequent value is not easily obtainable from that given value, a series of n values using a one-way coding function as taught by Chow to the system of Sharma in order store seed value than use to calculate the reference value, and storing the quantity of the fewer iterations.

As to claim 59, claim is rejected for the same reason as set forth in claim 58.

As to claim 60, claim is rejected for the same reason as set forth in claim 58.

Allowable Subject Matter

6. Claims 31-52 are allowed.

As to claim 31, Sharma discloses a method of authenticating a mobile node to a communication system, the communication system comprising a plurality of access nodes between which the mobile node is able to roam (page 4, par. [0054-0055], Chow discloses the method comprising: (a) generating a numerical chain comprising a series of values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value (page 9, par. [0165-0166]). However, either alone or combination of Sharma and Chow does not disclose that but the subsequent value is not easily obtainable from that given value; (b) each time that the mobile node seeks to authenticate itself to an access node, sending a value from the numerical chain from the mobile node to an access node to which the mobile node wishes to attach, the sent value preceding values in the chain already sent to access nodes; and (c) using the sent value at the access node to authenticate the mobile node on the basis of a value of the numerical chain preceding the sent value in the chain, the method further comprising, after each successful authentication, informing each of said plurality of access nodes that an authentication has been completed

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Quick (US Pub No: 2005/0257255) discloses "Local authentication of mobile subscribers outside their home systems".

Soliman (US Pub No: 2004/0184605) discloses "Information security via dynamic encryption with hash function".

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHUOC H. DOAN whose telephone number is 571-272-7920. The examiner can normally be reached on 9:30 AM - 6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, VINCENT HARPER can be reached on 571-272-7605. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/VINCENT P. HARPER/
Supervisory Patent Examiner, Art Unit 2617

/PHUOC DOAN/
04/10/08